Improved Security of Compound Mapping Algorithm for Image Watermarking

MILOS JOKSIC
John Naisbitt University
Graduate School of Computer Science
Bulevar umetnosti 29, Belgrade
SERBIA
joksic.035@gmail.com

EVA TUBA
University of Belgrade
Faculty of Mathematics
Studentski trg 16, Belgrade
SERBIA
etuba@ieee.org

MILAN TUBA
John Naisbitt University
Graduate School of Computer Science
Bulevar umetnosti 29, Belgrade
SERBIA
tuba@ieee.org

Abstract: Data transmitting and copying have become important problems when it comes to unauthorized data replication. Digital watermarking is one of the solutions which may be implemented to reduce unauthorized image replication. Compound mapping algorithm is used to embed and extract a watermark from the digital image. Due to the various security attacks, a security improvement is proposed. Our proposed algorithm was tested on standard benchmark images and it successfully protected images from attacks.

Key–Words: Visible image watermarking, Compound mapping, Digital image processing

1 Introduction

Internet and multimedia technologies have become part of everyday life as well as creating and using different digital data such as texts, images, videos or audio formats. Massive use of digital data enabled great benefits, but it also leaded to unauthorized replication problem. As a result of the problem of unauthorized replication of materials, stenography contributed to the development of watermarking, a way to protect them and preserve their authenticity [1]. Both of them rely on the concept of incorporating information into cover data media. Digital watermark protects the image from unauthorized copying and reproduction by embedding the original with additional data to indicate the owners of the copyright [2].

The three main factors that impact the overall quality of the copyright pattern are robustness, imperceptibility and capacity.

- **Robustness:** The removal or destruction of a watermark should be challenging, for robust is a method of watermark immunity that is designed to safeguard images against alteration and manipulation such as filtering, rotation, sailing, cropping, resizing etc.

- **Imperceptibility:** Implies that the quality of the original image should not be consumed by the existence of a watermark.

- **Capacity:** Incorporates procedures that help facilitate the embodiment of information. [3]

In addition, there are two main kinds of watermarks, visible and invisible. Visible watermarks [4], like those on company logos, are noticeable, that is, they are the first line of defense whose task is to clearly indicate that the material is copyrighted and prevent further violation while invisible watermarks cannot be easily noticed and they are situated in the periphery of the content and they can be used to validate ones copyright.

Image watermarking can be done in spatial or frequency domain. In the spatial domain an image is represented in form of a pixelated matrix [5]. Embedding of a watermark is done by directly changing the value of pixels, which implies a change of the corresponding color and other parameters of the pixel exactly in the area intended for the insertion of the watermark. These algorithms are simple to understand and use as well as less time consuming and can be further used on any type of image.

On the other hand, in the frequency domain the image is represented in the form of frequency [6]. Initially the original image is converted by a predefined transformation and then the watermark is embedded into the transformed image or into the transformation coefficients and finally, the inverse transform is performed to obtain the watermarked image. Most commonly used transformations are discrete cosine trans-

form (DCT), discrete wavelet transform (DWT) and discrete Fourier transform (DFT).

It is important to highlight that the significant part of the well watermarking process is extracting the watermark from the watermarked image. The extraction process implies the removal of watermark from an already watermarked image. This is a critical part of the entire process and that is exactly why security is always a question of the highest importance. [7]

Thanks to the freedom that internet provides, we are more vulnerable then ever from numerous of different kinds of attacks. One of the problems of these attacks is that by removing a watermark the attacker is able to facilitate distribution, commercialization, and other kinds of malversation. Therefore, it is essential that security should entail the protection against data alteration from various unauthorized users and attackers [8].

In order to stop data modification and to help to protect data from unapproved hackers and end-users, data security is mandatory. As a result of the expanding rise in data distribution rate over the internet, data security has acquired higher awareness over the years. Therefore, the development of internet security was necessary which would not only provide security against illegal use but safeguard against the attacks that would jeopardize the security as well. To prevent these kinds of attacks some methods and techniques were developed such as cryptography, stenography and digital image watermarking [9].

The most common types of attacks, in the digital image watermarking, are known as removal attacks. Extraction attackers endeavor to isolate the watermarked data from the data of the original image and remove only the watermark image, via the analysis and estimation of the watermark. Some examples of these kinds of attacks may include: collision attacks, compression attacks, certain filter operation or denoising [10].

One way to maintain security is through the use of secret keys, not only for detection but embedding processes as well. The three types of these keys are: private-key, detection-key and public-key. The purpose of these keys is to prevent the security attacks covered above, and provide the removal of the watermark only to the authorized personal that are in possession of the keys [11].

There are many different algorithms and techniques that use pseudo-randomized keys and some of these will be presented in the next section.

In this paper a method for securing compound-mapping algorithm is presented. This algorithm is proposed and tested on various images different in sizes and quality. Quality and security of proposed algorithm is measured with several standard metrics, such as primary different kinds of removal attacks.

The rest of the paper is organized as follows. In Section 2 literature review of algorithms for embedding and extracting watermark is presented. In Section 5 security improvement of algorithms for spatial domain is proposed. Section 4 contains the results obtained by our proposed algorithm. And finally Section 5 delivers a conclusion.

2 Literature Review

Today there is a numerous of techniques for image watermarking [13]. A great number of these techniques is widely used and some of them will be discussed in this section. However, a number of security attacks and vulnerabilities are on the rise and therefore there is a lot of space for improvement when it comes to watermarking. Digital watermarking is already widely used all over the world and many different approaches have been successfully used, but growing security attacks and the growing need for the use of this system on the increasing number of roads make this problem still popular for researchers.

In the [14] a simple method for digital image watermarking was presented. This method relies on EXIF metadata (camera model, date taken, copyright, etc.) which works as a watermark [15]. Even when the marked image has been intentionally modified, the original EXIF with selected information can mostly be recovered from the channel decoding process. Because it is easy to manipulate and modify EXIF data, this type of algorithm is less secure than others.

A more sophisticated and secure method for digital image watermarking, that relies on frequency domain was shown in [16]. It was based on joint DWT-DCT [17]. Against frequent signal processing attacks a more advanced robustness, along with imperceptibly, was maintained. Initially, in certain sub-bands of a 3-level DWT transformed of a host image, a binary watermarked image was embedded. Next, the PN-sequences of the watermark bits and the DCT transform of each selected DWT sub-band, were inserted in the coefficients of the matching DCT middle frequencies. During extraction stages, which maybe attacked, the watermarked image was first preprocessed through the use of sharpening and various kinds of filters. The similar approach, to the embedding process, was used to obtain the DCT middle frequen-

cies of each sub-band. Ultimately, an interaction was computed between PN-sequences and mid-band coefficients in order to determine watermarked bits. In conclusion, the results showed that the recommended method enhanced the performance of the watermarking algorithm which rely on the joint of DWT-DCT.

Two lossless visible watermarking algorithms were proposed in [18], pixel value matching algorithm (PVMA) and pixel position shift algorithm (PPSA). Since the embedding distortion of noticeable watermarking was generally greater than that invisible watermarking, lossless property was highlighted so as to preserve the fidelity of the signal following the watermark extraction. In PVMA, the objective intensity mapping function was used in order to watermark a visible logo. PPSA, on the other hand, made use of circular pixel shift so as to improve the visibility of the watermark in regions with high variance.

In addition to the PVMA and PPSA, there is an older and easier method of embedding the watermark known as least significant bit (LSB) [19]. The implementation of a watermark in the LSB pixels does not only allow easier implementation but it does not severely distort the image as well, although when it comes to attacks it lacks robustness against them. Through the selection of a subset of image pixels and the substitution of the least important bit of each of the selected pixels with the watermark bits, the embedding of a watermark is achieved. Furthermore, the watermark can be expanded all over the image or it may be located in the preferred positions of the image. However, as a result of these primitive techniques being not only vulnerable to attacks but highly sensitive to noise and common signal processing, the watermark can be easily destroyed.

A security improvement to the mentioned LSB technique is the use of a random key which is obtained by a pseudo-randomized number generation [20]. Random key is not a final security measure. It makes the removal of a watermark more difficult but not impossible.

In [21] a method which provides visible watermarking that does not impact the image quality, named compound mapping method. The proposed method used deterministic one-to-one mappings of image pixel values where $\boldsymbol{f}$ converts a set of numerical values of pixels P = p1, p2, . . . ,pm to another set W = w1, w2, . . ., wm that represents pixels with watermark on themselves. The original image can be recovered from previously watermarked image by using the corresponding reverse method. In order to maintain solid security level, set W was randomized therefore the extraction of a watermark without a key was impossible.

An innovative use of compound capping method for images in PNG format was presented in [22]. Advantage of the PNG format is that it has the additional A-alpha channel. In the A-alpha channel plane, those pixels which underly the ones that have been watermarked in the color channel plane will be appointed a unique alpha value. An additional advantage of this method was the fact that during the recovery process, the original watermark image was not required. In addition to all this, random generated numbers were used as a security measure to prevent the removal of the watermark without a key.

As mentioned above, there are very successful methods of image watermarking, but there is a lot of space for improvement. In the next section we propose our method for better security protection in the process of embedding and extracting watermark.

3 Our Proposed Method

As it was mentioned in the previous section, compound mapping methods usually use randomized keys in the process of watermark embedding. There is no precise explanation for the exact algorithm used to generate random numbers. In this paper, we propose using some concrete algorithm for generating pseudo-randomized numbers which will add more complexity to the numbers and keys which will disable the removal of the watermark due to the mentioned complexity.

Usage of the compound mapping for embedding or extracting the watermark to an image will be explained by using pseudo code.

Algorithm 1: Process of watermark embedding

Input: Color original (host) image I, a watermark L.
Output: Watermarked Image W.

1. Indicate P as a watermarking area before proceeding to select a set P of pixels from I where W is to be embedded. The set of pixel P depicts the values of pixels prior the watermark embedding process.
2. Designate the set of pixels equivalent to P in W by Q Q being the set of pixels which includes the values of the watermarked pixels.

3. For each pixel X which contains the value p in P, designate the equvivalent pixel in Q as Z, the value of the equivalent pixel y in L as l, and conduct the following steps:

   (a) Administer an evaluation technique so as to obtain a to be a value close to p, via the utilization of the values of the neighboring pixels of X (excluding x itself).

   (b) Appoint b to be the vale l

   (c) Map p to a new value

   $$q = F_b^{-1}(F_a(p))$$

   (d) Set the value of Z to be q.

4. Set the value of each remaining pixel in W, which is outside the region P, to be equal to that of the corresponding pixel in l.

Our proposed method includes pseudo-randomized numbers into Algorithm 1 in order to improve a security. The goal is to get more complex key on the part when pseudo-randomized numbers are generated so that can not be easily broken, which would lead to watermark removing.

Algorithm 2: Process of watermark extraction

Input: Watermarked image W, and a Watermark L
Output: Original (hosted) image R, recovered from W

1. Select the exact watermarking are Q in W as that which was selected in Algorithm 1 (Indicates the area where the watermark is located).

2. Appoint the value of each pixel in
   R, which is outside the region Q, to be identical to that of the corresponding pixel in W. Pixels outside the watermarked area are not changed, and thus retain the same values.

3. For each pixel Z with the value q in Q, designate the equivalent pixel in the recovered image R as x and the value of corresponding pixel Y in L as l, and conduct the following steps:

   (a) Attain the same value a as that derived in step *3a* of Algorithm 1 by administering the same estimation technique that was used there.

   (b) Set b to be the value l.

   (c) Restore p from q by setting

   $$p = F_a^{-1}(F_b(q))$$

   (d) Set the value of x to be p.

A efficient way to maintain higher security level, by using compound mapping algorithm mentioned above, is generate secret key from parameters a, and b, in the part of the watermark image embedding. These two parameters are practically integer values that contains values of the pixels range [0, 255], so there are many ways to randomize them or even encrypt, in order to avoid easy watermark removal.

4 Experimental results

For Experimental results, and demonstration on Compound Mapping algorithm we will use a standard test image widely used in a field of image processing.

Compound mapping method with our proposed method for security improvement proved to be efficient for image watermarking; simultaneously for embedding and extracting watermarks. In Fig. 1 is the previously mentioned standard test image. This image is used as a host image for embedding watermark.

Figure 1: Original image

In Fig. 2, the same image is presented with an embedded watermark using the formerly mentioned compound mapping algorithm with our proposed improved security. The process of watermark embedding

Figure 2: Image with watermark embedded

Figure 3: Image with watermark removed

was explained in Algorithm 1, which is further defined via the pseudo-code.

Figure 3 represents a watermarked image after the watermark extraction process, which can be likewise explained via the pseudo-code. As we can see, the quality of the image, which had gone through the processes of embedding and extraction, is almost the same as the original image showed in Fig. 1. Having tested our proposed algorithm on fifteen images, a conclusion was reached that the algorithm not only had good performances but it also preserved the original quality.

5 Conclusion

Security improvement of the compound mapping algorithm used both for embedding and extraction, was proposed in this paper. Security improvement is related to the parts of embedding as means of generating a secret key to prevent watermark removal via the various attacks. Thus, the watermark extraction process can only be successful with the use of the correct secret key. Compound mapping algorithm with our improvements was tested on standard benchmark images and the predicted results were met. Having in mind that we have discussed about the algorithm that works with the spatial domain, future research may include improvement of security in frequency domain and invisible watermarking method.

Acknowledgments: This research is supported by Ministry of Education, Science and Technological Development of Republic of Serbia, Grant No. III-44006.

References:

[1] M. Hussain and M. Hussain, "A survey of Image steganography techniques," *Citeseer*, 2013

[2] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, "Properties of digital image watermarking," in *Signal Processing and its Applications (CSPA), 2013 IEEE 9th International Colloquium on*. IEEE, 2013, pp. 235–240.

[3] B. L. Gunjal and R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 1, pp. 37–42, 2010.

[4] F.-H. Hsu, M.-H. Wu, C.-H. Yang, and S.-J. Wang, "Visible watermarking with reversibility of multimedia images for ownership declarations," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 247–268, 2014.

[5] A. K. Singh, N. Sharma, M. Dave, and A. Mohan, "A novel technique for digital image watermarking in spatial domain," in *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*. IEEE, 2012, pp. 497–501.

[6] G. D. Leena, S. S. Dhayanithy, and M. Hwang, "Robust image watermarking in frequency domain," *International Journal of Innovation and Applied Studies ISSN*, pp. 2028–9324, 2013.

[7] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," *Information sciences*, vol. 279, pp. 251–272, 2014.

[8] P. Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, pp. 1–4, 2012.

[9] P. Singh and R. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 9, pp. 165–175, 2013.

[10] H. K. Sunesh, "Watermark attacks and applications in watermarking," in *National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC)*, 2011.

[11] M. M. U. Bhaisare and V. R. Raut, "Generic lossless visible watermarking," *International Journal of scientific research and management (IJSRM)*, vol. 3, 2015.

[12] K. S. P. S. Nellore and P. M. SWAMY, "Generic lossless visible watermarking," *Int. J. of Engg. Sci. & Mgmt.(IJESM)*, vol. 3, no. 2, 2013.

[13] T. K. Araghi, A. B. A. Manaf, M. Zamani, and S. K. Araghi, "A survey on digital image watermarking techniques in spatial and transform domains," 2016.

[14] H.-C. Huang and W.-C. Fang, "Metadata-based image watermarking for copyright protection," *Simulation Modelling Practice and Theory*, vol. 18, no. 4, pp. 436–445, 2010.

[15] E. Kee, M. K. Johnson, and H. Farid, "Digital image authentication from JPEG headers," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1066–1075, 2011.

[16] S. A. Kasmani and A. Naghsh-Nilchi, "A new robust digital image watermarking technique based on joint DWT-DCT transformation," in *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2. IEEE, 2008, pp. 539–544.

[17] K. Deb, M. S. Al-Seraj, M. M. S. Kowsar, and I. H. Sarkar, "A joint DWT-DCT based watermarking technique for avoiding unauthorized replication," in *Strategic Technology (IFOST), 2012 7th International Forum on*. IEEE, 2012, pp. 1–5.

[18] S.-K. Yip, O. C. Au, C.-W. Ho, and H.-M. Wong, "Lossless visible watermarking," in *2006 IEEE International Conference on Multimedia and Expo*. IEEE, 2006, pp. 853–856.

[19] A. Bamatraf, R. Ibrahim, M. Salleh, and N. Mohd, "A new digital watermarking algorithm using combination of Least Significant Bit (LSB) and Inverse bit," *arXiv preprint arXiv:1111.6727*, 2011.

[20] P. K. Sharma, "Rajni: Analysis of image watermarking using least significant bit algorithm," *International Journal of Information Sciences and Techniques (IJIST) Vol*, vol. 2, 2012.

[21] T.-Y. Liu and W.-H. Tsai, "Generic lossless visible watermarkinga new approach," *IEEE transactions on image processing*, vol. 19, no. 5, pp. 1224–1235, 2010.

[22] C.-W. Lee and W.-H. Tsai, "A new lossless visible watermarking method via the use of the PNG image," 2012.